



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/923,574	08/07/2001	Ronald O'Neal Edmark	AUS920010185US1	2691

35525 7590 03/09/2005

IBM CORP (YA)
C/O YEE & ASSOCIATES PC
P.O. BOX 802333
DALLAS, TX 75380

EXAMINER

NGUYEN, MINH DIEU T

ART UNIT PAPER NUMBER

2137

DATE MAILED: 03/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<p align="center">Office Action Summary</p>	<p>Application No.</p> <p align="center">09/923,574</p>	<p>Applicant(s)</p> <p align="center">EDMARK ET AL.</p>	
	<p>Examiner</p> <p align="center">Minh Dieu Nguyen</p>	<p>Art Unit</p> <p align="center">2137</p>	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 August 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-22 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| <p>1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)</p> <p>2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)</p> <p>3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
 Paper No(s)/Mail Date <u>03/06/2003</u>.</p> | <p>4) <input type="checkbox"/> Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____</p> <p>5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)</p> <p>6) <input type="checkbox"/> Other: _____</p> |
|--|---|

DETAILED ACTION

1. Claims 1-22 are pending.

Claim Objections

2. Claims 1 and 4-5 are objected to because of the following informalities:
 - a) As to claim 1 on page 14, line 7, "the the incoming request" should be "the incoming request".
 - b) As to claim 4 on page 14, line 22, "the when the request" should be "the request".
 - c) As to claim 5 on page 15, line 6, "a intrusion" should be "an intrusion" and line 9, "the the incoming request" should be "the incoming request".Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Coley et al. (5,826,014).

a) As to claims 1, 9 and 13, Coley discloses firewall system (i.e. server system) for protecting network elements connected to a public network comprising one or more source servers that store information (Fig. 2, elements 216, 218); a first server (Fig. 2, element 210), communicatively coupled to the one or more source servers and to the network; that receives the incoming request from the network (col. 7, lines 16-18) and the first server testing the incoming request (col. 7, lines 35-39) for an indicia (col. 6, lines 34-39; col. 8, lines 6-9) contained within the request that the request is not proper for the source servers to respond to the request (col. 7, lines 56-57), and passing the incoming request to the one or more source servers when the incoming request is valid (col. 9, lines 13-18).

b) As to claims 2, 6, 11 and 15, Coley discloses the one or more source servers transmitting information to the first server in response to the incoming request and the first server re-transmitting the information to the user (col. 12, lines 7-19).

c) As to claims 3 and 7, Coley discloses the first server does not pass the incoming request to the one or more source servers when the incoming request is an indicia that the request is not proper for the source servers to respond to the request (Figs. 4A/B).

d) As to claims 4, 8, 12 and 16, Coley discloses the incoming request is determined to be not proper when the request is for access to a particular resource (col. 10, lines 53-55).

e) As to claim 5, Coley discloses a computing system that preprocesses and monitors incoming requests for information from a user over network (Fig. 2), the

Art Unit: 2137

information stored on one or more source servers communicatively coupled to the computing system (Fig. 2, elements 216, 218), the computing system comprising a network input port that receives the request (Fig. 2, element 206); a source server port (Fig. 2, element 210), communicatively coupled to the one or more source servers, that transmits information to and from the source servers; an intrusion detection mechanism communicatively coupled to the network input port (col. 7, lines 35-37); the intrusion detection mechanism receiving the incoming request from the network and checking the incoming request for indicia of an improper request from information associated with the incoming request (col. 7, line 64 to col. 8, line 16); the intrusion detection mechanism transmitting the incoming request to the one or more servers when the indicia associated with the incoming request is valid (col. 9, lines 13-18).

f) As to claims 10 and 14, Coley discloses the step of determining is performed by a software resident on the computing system (col. 13, lines 46-56).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 17, 17, 20 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al. (5,826,014) in view of Rowland (6,405,318).

a) As to claim 17, Coley discloses firewall system (i.e. server system) for protecting network elements connected to a public network comprising one or more source servers that store information (Fig. 2, elements 216, 218); a first server (Fig. 2, element 210), communicatively coupled to the one or more source servers and to the network; that receives the incoming request from the network (col. 7, lines 16-18), the first server detecting an intrusion of the incoming request (col. 7, lines 54-55; line 64 to col.. 8, line 16) and based on indicia (col. 6, lines 34-39; col. 8, lines 6-9) of the incoming request being proper, such indicia being associated with the incoming request, and the first server passing the incoming request to the one or more source servers when the indicia associated with the incoming request indicates that the incoming request is proper (col. 9, lines 13-18).

However, Coley does not disclose the first server detecting an intrusion of the incoming request in the context of prior requests.

Rowland discloses a computer implemented intrusion detection system and method that monitors a computer system in real-time for activity indicative of attempted or actual access by unauthorized persons or computers comprising the first server detecting an intrusion of the incoming request in the context of prior requests (Abstract).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of detecting an intrusion of the incoming request in the context of prior requests in the system of Coley as Rowland teaches so as to effectively detect intrusions as they occur.

b) As to claim 19, Rowland discloses the context of prior requests comprises requests for different information from a common computing device coupled over the network (col. 6, lines 36-49).

c) As to claim 20, Rowland discloses the context of prior requests is based on a number of requests for the same information (col. 5, lines 10-15).

d) As to claim 22, Rowland discloses the context of prior requests is based on a number of requests for information from a particular IP address in a particular amount of time (col. 9, lines 21-24).

7. Claims 18 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coley et al. (5,826,014) in view of Rowland (6,405,318) and further in view of Bernhard et al. (6,275,942).

a) As to claim 18, Coley and Rowland do not disclose the context of prior requests comprises requests for the same information.

Bernhard discloses a system, method and computer program product for automatic response to computer system misuse comprising the context of prior requests comprises requests for the same information (col. 1, lines 63-67).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of comprising requests for the same information in the context of prior requests in the system of Coley and Rowland, as Bernhard teaches so as to effectively detect intrusions as they occur.

Art Unit: 2137

b) As to claim 21, Bernhard discloses the context of prior requests is based on a number of requests from a particular IP address (col. 8, lines 59-65).

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873. The examiner can normally be reached on M-F 6:00-2:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on 571-272-3868. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Minh Dieu Nguyen
Examiner
Art Unit 2137

mdn
3/3/05



**ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER**